JJ
Corresponds to
IW

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06, 12/22, G07C 9/00 — A1

(11) International Publication Number: WO 99/55052

(43) International Publication Date: 28 October 1999 (28.10.99)

(21) International Application Number: PCT/US99/06206

(22) International Filing Date: 22 March 1999 (22.03.99)

(30) Priority Data:
09/063,630 20 April 1998 (20.04.98) US

(71) Applicant *(for all designated States except US)*: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PAL01-521, Palo Alto, CA 94303 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: GUPTA, Amit [-/US]; 901 San Antonio Road, Palo Alto, CA 94303 (US). PERLMAN, Radia, J. [-/US]; 10 Huckleberry Lane, Acton, MA 01720 (US).

(74) Agents: HOLLINGER, Joseph, K. et al.; Graham & James LLP, 600 Hansen Way, Palo Alto, CA 94304-1043 (US).

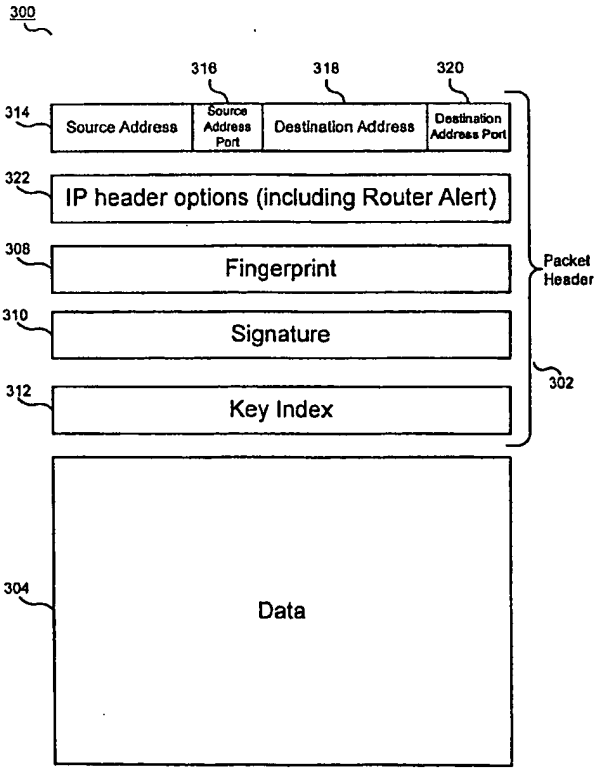
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR USING DIGITAL SIGNATURES TO FILTER PACKETS IN A NETWORK

(57) Abstract

A method and apparatus for filtering packets uses digital signatures to filter packets in a network. A filter point, such as a router or firewall to an intranet, receives a packet including a header, detects the existence of a signature in the header, tests the validity of the signature using a public key, and forwards the packets in accordance with the validity of the signature. A sender uses a private key obtained from an owner to generate the signature, which is created by encrypting a fingerprint which corresponds to the data in the packet. Public keys are created by an owner which installs them in a domain name system or a certification server. Private keys are also created by the owner but are disseminated only to authorized senders. A method and apparatus for sending packets stores a private key in a memory of the data processor, generates a signature using the private key, installs the signature into a header of a packet; and sends the packet.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Method and Apparatus for Using Digital Signatures to Filter Packets in a Network

FIELD OF THE INVENTION

The present invention relates generally to network communications. More specifically, the present invention is a method and apparatus for using digital signatures to filter packets in a network.

BACKGROUND OF THE INVENTION

Internet protocol (IP) Multicasting is a form of network communication in which a single message is sent to multiple destinations at once. A multicast group owner sets up a multicast group address. Senders and receivers may join the group by accessing the group address.

One problem with IP multicast is that it allows unauthorized senders to transmit to the multicast group, requiring the end host system to keep state and to process packets which are not authorized to be sent to the group. The packets are transmitted by the unauthorized sender and forwarded by routers to the end host. Routers are systems which can be used to forward packets between networks.

One solution to this problem is for the group owner to encrypt the session and require authorized members to obtain a group key in order to decrypt the data. However, this mechanism does not prevent denial of service attacks where unauthorized senders from a network on one side of a router or a firewall transmit numerous IP messages to an end host in a network on the other side of the router or firewall. The router or firewall passes the packets from the network where the sender is located to the network where the end host is located, without processing the packets. The end host receives and processes each packet to determine whether the sender may join the encrypted session. If the sender is not authorized to join the session, the end host denies service to that sender. A malicious user, in what is called a denial of service attack, may send numerous unauthorized messages to an end host system on the other side of a router or a firewall. Even though the malicious user is not authorized to access the system, it can cause a network bottleneck because the end host at the other side of the router or firewall

must process all of the incoming messages to determine whether the sender may join the encrypted session, thereby using up network bandwidth and resources.

SUMMARY OF THE INVENTION

Consistent with the present invention, a method and apparatus for using digital signatures filters packets in a network in order to avoid wasting router bandwidth and resources on processing packets associated with unauthorized senders.

An embodiment consistent with the present invention includes a method and apparatus for filtering packets, performed by a data processing system, which comprises the steps of receiving a packet including a header; detecting the existence of a signature in the header, and forwarding the packet in accordance with the validity of the signature. The data processing system that performs these steps may be, for example, a router or a firewall. An embodiment consistent with the present invention may be implemented as a computer program product or as a computer data signal embodied in a carrier wave. An embodiment consistent with the present invention also includes a method and apparatus for sending packets, performed by a data processing system, which comprises the steps of storing a private key in a memory of the data processor, generating a signature using the private key, installing the signature into a header of a packet, and sending the packet. . An embodiment consistent with the present invention may be implemented as a computer program product or as a computer data signal embodied in a carrier wave.

An owner disseminates private keys to the senders. When there are numerous keys, the keys may be stored in indexed tables. A sender signs the packet using the one of the private keys. A router or a firewall then determines the validity of the signature by checking the signature using the public key. If the signature is valid, the router or firewall forwards the packet. Packets having an invalid signature are discarded.

The method for signing the packet may include creating a fingerprint corresponding to the data and encrypting the fingerprint using a private key to yield a signature. The method for checking the signature may include decrypting the

fingerprint using a public key and comparing the decrypted fingerprint to a newly created fingerprint of the data.

An embodiment consistent with the present invention also includes a method for filtering packets, performed by a data processing system, which comprises the steps of receiving a plurality of packets, each of which includes a header, determining a number of packets received from a particular source, detecting the existence of a signature in the header, and forwarding the packet in accordance with the validity of the signature and with whether a router limit has been exceeded. The router limit may be associated with a number of packets per predetermined set of senders in order to limit the size of the group of authorized senders. The router limit also may be associated with a predetermined period of time to limit the rate at which senders transmit packets to the router.

Advantages of the invention will be set forth, in part, in the description that follows and in part, will be understood by those skilled in the art from the description or may be learned by practice of the invention. The advantages of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims and equivalents.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments consistent with the present invention and, together with the description, serve to explain the principles of the invention.

Fig. 1 is a diagram of a network in accordance with an embodiment consistent with the present invention.

Figs. 2(a) and 2(b) are diagrams of data processing systems in accordance with an embodiment consistent with the present invention.

Fig. 3 is a diagram showing a format of a packet in accordance with an embodiment consistent with the present invention.

Fig. 4 is a diagram of a network in which a public key of an owner is placed in a DNS server.

Fig. 5 is a flow chart showing steps performed by an owner in accordance with an embodiment consistent with the present invention to create and distribute keys.

Fig. 6 is a flow chart showing steps performed by a sender in accordance with an embodiment consistent with the present invention to sign packets.

Fig. 7 is a flow chart showing steps performed by a router or a firewall in accordance with an embodiment consistent with the present invention to determine whether to forward packets.

Fig. 8 is a flow chart showing steps performed by a router in accordance with an embodiment consistent with the present invention to filter packets in accordance with a router limit.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to embodiments consistent with the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

Fig. 1 is a diagram 100 of an embodiment consistent with the present invention which shows a network 102 containing a router 104. An owner 106 disseminates private key S_1 to senders 108 and 110, as shown by arrows 116 and 118. Owner 106 disseminates the private keys by a known method. These private keys are also known as secret keys or signature keys. Owner 106 may store a pair of keys, one for send and one for listen access, or alternatively, the owner may create a table of keys in which the table entries are accessed using an index corresponding to a particular key.

Sender 110 receives its private key S_1 from owner 106, as shown by arrow 118. When sender 110 sends a multicast packet, it generates a fingerprint corresponding to data contained in a packet, and then uses the sender's private key to encrypt the fingerprint. The encrypted fingerprint is a unique signature which is used to identify that the sender has authorization to send the packet to the multicast group. The sender includes the fingerprint and signature with the remaining packet contents and then sends the packet.

Router 104 receives the packet from sender 108, 110, as shown by arrows 128, 124, and processes the packet to determine whether to forward the packet. This process is described in further detail below. If a signature is required, exists, and is valid, then router 104 forwards the packet to receiver 112, 114, as shown by arrows 130, 126.

Fig. 2(a) is a block diagram of a data processing system 200 showing an embodiment consistent with the present invention. Data processing system 200 includes router or firewall system 206, input device 208, output device 210, computer readable medium 212, computer readable medium input device 214 and a network connection 237. Router or firewall system 206 includes processor 202 and storage 204 such as a memory.

Storage 204 contains filtering software 218 and public key table 216. Public key table 216 contains one or more public keys of the senders which were generated by owner 106. Three public keys P_1, P_2, and P_3 217 and their associated indexes 215 are shown in public key table 216. Storage 204 also contains a flag 213 which determines whether this router requires a signature in the multicast packet.

The public keys are obtained from the domain name system (DNS) 412, a certification server (not shown), or any other appropriate key distribution scheme, and are stored in public key table 216. Filtering software 218 uses an appropriate key from public key table 216 to check the validity of the signature contained in the header of an incoming packet. If the signature is valid, then router 206 forwards the packet to receivers 112, 114, as shown by arrows 130, 126. Otherwise, the packet may be discarded. This process is described in further detail below.

A person of ordinary skill in the art will understand that data processing system 200 may also contain additional information, such as input/output lines; input devices, such as a keyboard, a mouse, and a voice input device; and display devices, such as a display terminal. Input device 208 may be a floppy disk drive, CD ROM reader, or DVD reader, that reads computer instructions stored on a computer readable medium, such as a floppy disk, a CD ROM, or a DVD drive. Data processing system 200 also may include application programs, operating systems, data, etc., which are not shown in the figure for the sake of clarity. It also will be

understood that data processing system 200 may also include numerous elements not shown, such as disk drives, keyboards, display devices, network connections, additional memory, additional CPUs, LANs, input/output lines, etc.

In the following discussion, it will be understood that the steps of methods and flow charts discussed preferably are performed by an appropriate processor 202 executing instructions stored in storage 204. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

The instructions in storage 204 may be read from computer-readable medium 212. Execution of sequences of instructions contained in storage 204 causes processor 202 to perform the process steps described herein. In alternative embodiments consistent with the present invention, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments consistent with the present invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to a processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as a storage device. Volatile media includes dynamic memory. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise a bus within a computer. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

Common forms of computer-readable media include, for example a floppy disk, a flexible disk, a hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, paper tapes, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to a processor for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to the computer system can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector coupled to a bus can receive the data carried in the infra-red signal and place the data on the bus. The bus carries data to main memory, from which a processor retrieves and executes the instructions. The instructions received by main memory may optionally be stored on a storage device either before or after execution by a processor. The instructions can also be transmitted via a carrier wave in a network, such as a LAN, a WAN, or the internet.

Fig. 2(b) is a block diagram of a data processing system 219 showing an embodiment consistent with the present invention. Data processing system 219 includes sender system 224, input device 226, output device 228, computer readable medium 230, computer readable medium input device 232, and a network connection 238. Sender system 224 includes processor 220 and storage 222, such as a memory. Sender software 234 and private key table 236 containing indexes 235 to private keys S_1, S_2, and S_3 237 are contained within storage 222.

Fig. 3 is a diagram showing a format of a packet format 300 which contains an IP header 302 and data 304. IP header 302 contains an IP header options field 322, a fingerprint (also called a digest or a message digest) 308, a signature (also called a signed fingerprint or encrypted message digest) 310, and a key index 312.

The key index indicates an entry in a key table where a plurality of keys are stored. If only one key is stored, the use of the key index is optional, for example if P_1 was the only key stored in storage 204 in the router. The index is used to retrieve a particular key from the table. In public key table 216, indexes 215 point to public keys 217. For example, key P_1, is stored in public key table 216 and is associated with an index having a value of 1. This value is stored in key index 312 in the packet header. Similarly, key P_2, is associated with an index having a value of 2, and key P_3, is associated with an index having a value of 3.

IP header 302 also includes a source address 314, a source address port 316, a destination address 318, and a destination address port 320. IP header options 322 include a router alert option. The purpose of the router alert option is to alert routers to examine the contents of an IP packet more closely and to provide backward compatibility with other network protocols.

The router alert option format contains a 4-byte field in which two of the bytes contain a two octet code indicating whether the router should examine the packet. If the value of the octet is zero, the packet is examined. If the value of the octet is anything else, the packet is not examined. The IP Router Alert Option is described more fully in Request for Comments (RFC) 2113 written by D. Katz in February 1997, which is herein incorporated by reference to the extent that it is not inconsistent with the present invention. It should be understood that packet format 300 includes other fields not shown in the figure for the sake of clarity.

Fig. 4 shows a network 102 in a system generally designated 400, an owner 106, a router 104, and a DNS server 412. DNS server 412 is a general-purpose distributed data query service used for translating hostnames into IP addresses. DNS server 412 includes a DNS table 408. Owner 106 installs DNS table entry 406 into DNS table 408. Table entry 406 includes both a public key P_1 and its associated IP address. Router 104 requests DNS table entry 406 from DNS server 412 in order to retrieve public key P_1.

In an embodiment consistent with the present invention, owner 106 creates and distributes public and private keys. An embodiment consistent with this method is shown in Fig. 5 and generally designated 500. In step 502, owner 106 creates several public and private key pairs for a multicast and stores them in indexed tables. In step 504, owner 106 obtains a private multicast address. Next, in step 506, owner 106 installs the public keys for the multicast. Owner 106 may install the public keys in the DNS server 412 or in a certification server. After installing the public keys, owner 106 distributes private (secret) keys to authorized senders, in step 508. Note that owner 106 may change which senders are authorized by sending a replacement key to a new set of authorized senders and by disallowing use of the current key. If there are multiple private keys, an index is associated with each key. As shown in Fig. 2, both public key table 216 (in the DNS server) and

private key table 236 (in the sender) can be indexed. At step 510, the sender is ready to begin.

In an embodiment consistent with the present invention, sender 108 signs a packet before sending it. An embodiment consistent with this method is shown in Fig. 6 and generally designated 600. In step 602, sender 108 obtains the private key and key index 312 (assuming there are multiple keys) from owner 106. This step is performed separately at some time before steps 606 - 616. Steps 606 - 616 send a signed multicast message. In step 606, sender 208 generates a fingerprint or digest 308 corresponding to data 304 in packet format 300. Methods for generating fingerprint 308 include MD5 and EC2/4 which are described in B. Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996, Chapter 18.5, which is herein incorporated by reference to the extent that it is not inconsistent with the present invention.

Next, in step 608, sender 108 creates signed fingerprint 310 by encrypting fingerprint 308 with the private key. The encryption may be implemented by a number of suitable encryption methods such as RSA, which is described which is in B. Schneier, Applied Cryptography, John Wiley & Sons, Inc., 1996, Chapter 19.3, which is herein incorporated by reference to the extent that it is not inconsistent with the present invention. This step is also known as signing the digest. Signed fingerprint 310 may be referred to as the signature. In step 609, sender 108 decides what to use for index 312. After creating signature 310 and deciding on an index, sender 108, in step 610, combines fingerprint 308, signature 310, index 312, and data 304 into one packet. Sender 108 then multicasts the packet in step 612. In step 614, sender 108 checks to find out if it has finished processing packets. If yes, then processing is over, step 616. If not, then sender 108 begins processing the next packet in step 604.

An embodiment consistent with the present invention, includes a "logical place" called a "filter point" which filters receive packets. The filter point receives a packet including header and data, detects the existence of a signature in the header, and forwards the packet in accordance with the validity of the signature. A filter point may be, for example, a router 104 or a firewall of an intranet. An embodiment consistent with this method is shown in the flow chart of Fig. 7 and generally

designated 700. In step 702, router 104 receives a packet having format 300. The packet is received from one of a sender 108, 110.

In step 704, router 104 determines whether packet format 300 contains a signature 310 by inspecting the router alert in IP header options field 322. If no signature 310 exists in packet format 300, router 104 then determines, in step 706, whether a signature is required. If a signature is not required, in step 708, router 104 forwards the packet. However, if a signature is required, and no signature is present, router 104 discards the packet, step 710. Router 104 preferably determines whether a signature is required by checking a flag 213 in storage 204. The flag may be set by any appropriate source.

If a signature 310 exists in packet format 300, router 104 then determines whether it has a valid public key corresponding to a valid key index, if applicable, in step 712. If router 104 does not have the public key, then it gets the public key from the Domain Name Server (DNS) 412, or from a certification server in step 714. Once router 104 has the public key, it uses the public key to check signature 310 in step 716. This checking step is done by decrypting the signature 310 to yield a decrypted fingerprint. If the decrypted fingerprint equals fingerprint 308 in the packet, then the signature is valid. Router 104 then determines whether signature 310 is valid by comparing the decrypted fingerprint and the fingerprint 308. If the two values match, the signature is valid. If signature 310 is valid, router 104 forwards the packet in step 720. If signature 310 is not valid, then router 104 discards the packet, in step 722.

An embodiment consistent with the present invention includes a router which filters packets in accordance with a predetermined router limit. An embodiment consistent with this method is shown in the flow chart of Fig. 8 and generally designated 800. At the start of this method, step 802, a predetermined router limit exists. This predetermined limit may be, for example, a rate at which the router may receive packets from a particular source or sender. Such a predetermined rate is useful in preventing denial of service attacks in which an unauthorized sender sends numerous unauthorized packets to the router.

First the router receives a packet, in step 804, and then in step 806, determines the particular source of the received packet. The number of packets

received from the source during the predetermined time period, i.e. the rate at which packets from this source are being received is determined in step 808. The router checks the router limit in step 810 by checking whether the maximum rate for the particular source has been exceeded. If the rate limit has been exceeded, the router discards the packet, in step 820. Otherwise, if the rate limit has not been exceeded, the router detects and checks the signature and routes the packet accordingly in step 812. See steps 704-722 of Fig. 7 above for more detail.

Other embodiments consistent with the present invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope of the invention being indicated by the following claims and equivalents.

WHAT IS CLAIMED IS:

1. A method of filtering packets, performed by a data processor, comprising the steps of:

receiving a packet including a header;

detecting the existence of a signature in the header; and

forwarding the packet in accordance with the validity of the signature.

2. The method of claim 1, wherein the steps of claim 1 are performed by a filter point and further comprising the step of disseminating a public/private key pair to, respectively, the filter point and a sender.

3. The method of claim 2, wherein the public keys and the private keys are stored in indexed tables.

4. The method of claim 1, wherein the step of forwarding the packet includes the step of discarding packets having an invalid signature.

5. The method of claim 1, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a router, using a public key of the sender.

6. The method of claim 1, wherein the data processing system is a firewall.

7. The method of claim 1, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a firewall, using a public key of the sender.

8. The method of claim 7, further including the steps, performed by the sender, to sign the packet, of:

creating a fingerprint corresponding to the data; and

encrypting the fingerprint using the sender's private key to yield the signature.

9. The method of claim 8, wherein the step of checking the signature includes the steps of:

decrypting the fingerprint using a public key of the sender; and

comparing the decrypted fingerprint to a fingerprint of the data.

10. A method of claim 1, further comprising:

determining a number of packets received in a predetermined time period from the source;

forwarding the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

11. The method of claim 10 wherein the router limit is associated with a number of packets per minute.

12. The method of claim 10 wherein the router limit is associated with a predetermined set of senders.

13. An apparatus that filters packets, comprising:

circuitry configured to receive a packet including a header;

circuitry configured to detect the existence of a signature in the header; and

circuitry configured to forward the packet in accordance with the validity of the signature.

14. The apparatus of claim 13, further comprising circuitry configured to disseminate a public/private key pair to, respectively, a filter point and a sender.

15. The apparatus of claim 14, wherein the public keys and the private keys are stored in indexed tables.

16. The apparatus of claim 13, wherein the circuitry configured to forward the packet further includes circuitry configured to discard packets having an invalid signature.

17. The apparatus of claim 13, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a router, using a public key of the sender.

18. The apparatus of claim 13, wherein the data processing system is a firewall.

19. The apparatus of claim 13, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a firewall, using a public key of the sender.

20. The apparatus of claim 19, further including:

circuitry configured to create a fingerprint corresponding to the data; and

circuitry configured to encrypt the fingerprint using the sender's private key to yield the signature.

21. The apparatus of claim 20, wherein the circuitry configured to check the signature further includes:

circuitry configured to decrypt the fingerprint using a public key of the sender; and

circuitry configured to compare the decrypted fingerprint to a fingerprint of the data.

22. A apparatus of claim 13, further including:

circuitry configured to determine a number of packets received in a predetermined time period from the source;

circuitry configured to detect the existence of a signature in the header; and

circuitry configured to forward the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

23. The apparatus of claim 22 wherein the router limit is associated with a number of packets per minute.

24. The apparatus of claim 22 wherein the router limit is associated with a predetermined set of senders.

25. An apparatus for filtering packets, comprising:

means for receiving a packet including a header;

means for detecting the existence of a signature in the header; and

means for forwarding the packet in accordance with the validity of the signature.

26. A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for filtering packets in a network that includes one or more systems, the computer program product including:

computer readable program code devices configured to cause a computer to receive a packet including a header;

computer readable program code devices configured to cause a computer to detect the existence of a signature in the header; and

computer readable program code devices configured to cause a computer to forward the packet in accordance with the validity of the signature.

27. The computer program product of claim 26, further comprising computer readable program code devices configured to disseminate a public/private key pair to, respectively, a filter point and a sender.

28. The computer program product of claim 27, wherein the public keys and the private keys are stored in indexed tables.

29. The computer program product of claim 26, wherein the computer readable program code devices configured to forward the packet further include computer readable program code devices configured to discard packets having an invalid signature.

30. The computer program product of claim 26, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a router, using a public key of the sender.

31. The computer program product of claim 26, wherein the data processing system is a firewall.

32. The computer program product of claim 26, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a firewall, using a public key of the sender.

33. The computer program product of claim 32, further comprising:

computer readable program code devices configured to create a fingerprint corresponding to the data; and

computer readable program code devices configured to encrypt the fingerprint using the sender's private key to yield the signature.

34. The computer program product of claim 33, wherein the computer readable program code devices configured to check the signature further include:

computer readable program code devices configured to decrypt the fingerprint using a public key of the sender; and

computer readable program code devices configured to compare the decrypted fingerprint to a fingerprint of the data.

35. A computer program product of claim 26, further comprising:

computer readable program code devices configured to determine a number of packets received in a predetermined time period from the source;

computer readable program code devices configured to forward the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

36. The computer program product of claim 35 wherein the router limit is associated with a number of packets per minute.

37. The computer program product of claim 35 wherein the router limit is associated with a predetermined set of senders.

38. A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by a processor, cause said processor to filter packets by performing the steps of:

executing a computer program to receive a packet including a header;

executing the computer program to detect the existence of a signature in the header; and

executing the computer program to forward the packet in accordance with the validity of the signature.

39. The method of claim 38, wherein the steps of claim 1 are performed by a filter point and further comprising the step of disseminating a public/private key pair to, respectively, the filter point and a sender.

40. The method of claim 39, wherein the public keys and the private keys are stored in indexed tables.

41. The method of claim 38, wherein the step of forwarding the packet includes the step of discarding packets having an invalid signature.

42. The method of claim 38, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a router, using a public key of the sender.

43. The method of claim 38, wherein the data processing system is a firewall.

44. The method of claim 38, wherein the packet is signed by a sender using a private key of the sender and wherein the validity of the signature is determined by checking the signature, by a firewall, using a public key of the sender.

45. The method of claim 44, further including the steps, performed by the sender, to sign the packet, of:

creating a fingerprint corresponding to the data; and

encrypting the fingerprint using the sender's private key to yield the signature.

46. The method of claim 45, wherein the step of checking the signature includes the steps of:

decrypting the fingerprint using a public key of the sender; and

comparing the decrypted fingerprint to a fingerprint of the data.

47. A method of claim 38, further comprising:

determining a number of packets received in a predetermined time period from the source;

detecting the existence of a signature in the header; and

forwarding the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

48. The method of claim 47 wherein the router limit is associated with a number of packets per minute.

49. The method of claim 47 wherein the router limit is associated with a predetermined set of senders.

50. A method for sending packets, performed by a data processor, comprising the steps of:

storing a private key in a memory of the data processor;

generating a signature using the private key;

installing the signature into a header of a packet; and

sending the packet.

51. An apparatus that sends packets, comprising:

circuitry configured to store a private key in a memory of the apparatus;

circuitry configured to generate a signature using the private key;

circuitry configured to install the signature into a header of a packet; and

circuitry configured to send the packet.

52. An apparatus for sending packets, comprising:

means for storing a private key in a memory of the apparatus;

means for generating a signature using the private key;

means for installing the signature into a header of a packet; and

means for sending the packet.

53. A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for sending packets in a network that includes one or more systems, the computer program product including:

computer readable program code devices configured to cause a computer to store a private key in a memory;

computer readable program code devices configured to cause a computer to generate a signature using the private key;

computer readable program code devices configured to cause a computer to install the signature into a header of a packet; and

computer readable program code devices configured to cause a computer to send the packet.

54. A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by a processor, cause said processor to send packets by performing the steps of:

executing a computer program to store a private key in a memory;

executing the computer program to generate a signature using the private key;

executing the computer program to install the signature into a header of a packet; and

executing the computer program to send the packet.

55. An apparatus that filters packets, comprising:

circuitry configured to receive, from a source, a packet including a header;

circuitry configured to determine a number of packets received in a predetermined time period from the source;

circuitry configured to detect the existence of a signature in the header; and

circuitry configured to forward the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

56. An apparatus for filtering packets, comprising:

means for receiving, from a source, a packet including a header;

means for determining a number of packets received in a predetermined time period from the source;

means for detecting the existence of a signature in the header; and

means for forwarding the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

57. A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for filtering packets in a network that includes one or more systems, the computer program product including:

computer readable program code devices configured to cause a computer to receive, from a source, a packet including a header;

computer readable program code devices configured to cause a computer to determine a number of packets received in a predetermined time period from the source;

computer readable program code devices configured to cause a computer to detect the existence of a signature in the header; and

computer readable program code devices configured to cause a computer to forward the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

58. A computer data signal embodied in a carrier wave and representing sequences of instructions which, when executed by a processor, cause said processor to filter packets by performing the steps of:

executing a computer program to receive, from a source, a packet including a header;

executing the computer program to determine a number of packets received in a predetermined time period from the source;

executing the computer program to detect the existence of a signature in the header; and

executing the computer program to forward the packet in accordance with the validity of the detected signature and whether the number of packets received in the predetermined time period from the source has exceeded a router limit for the particular source.

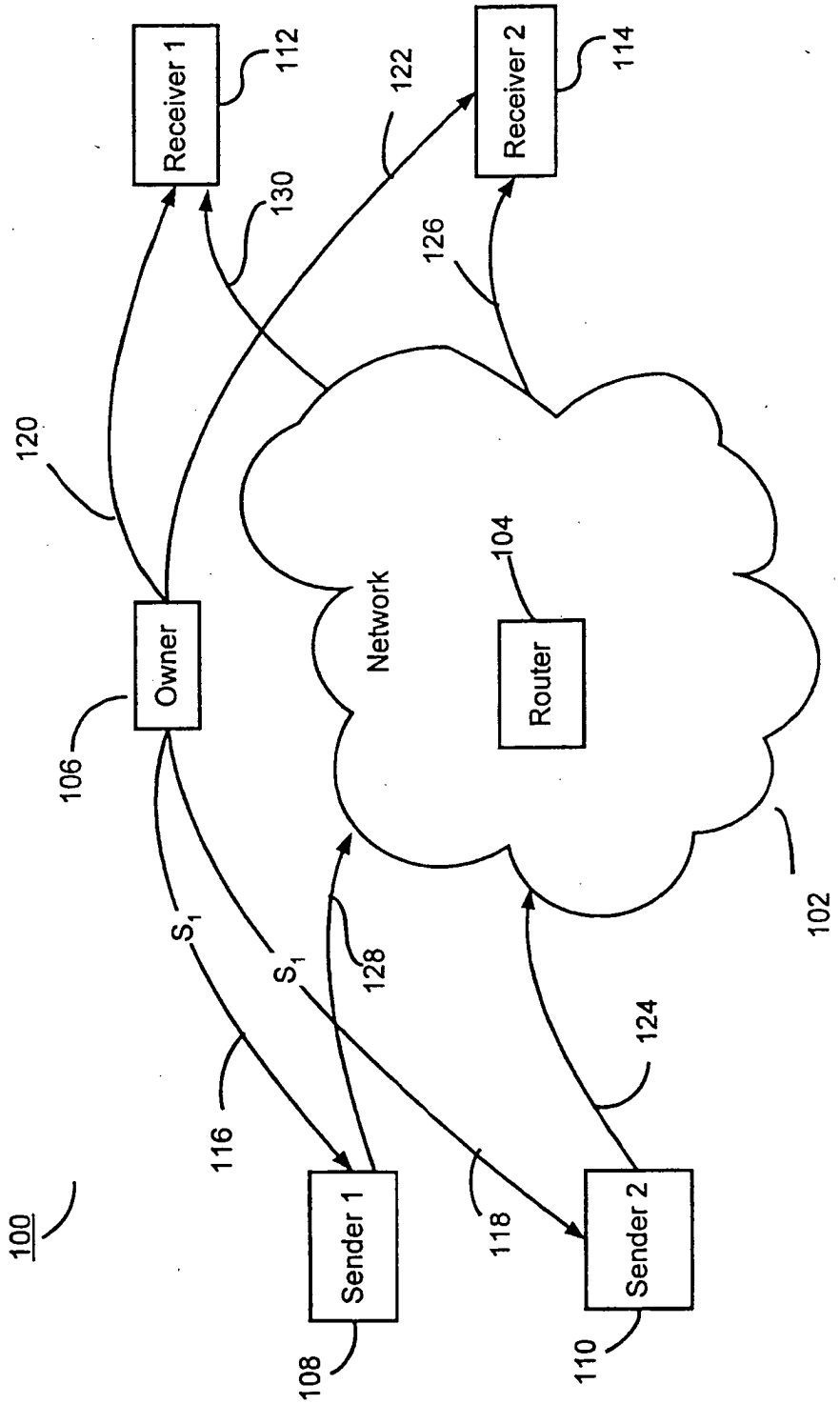

Receiver 1
112
Receiver 2
114
122
130
126
120
Network
104
Router
Owner
106
S_1
S_1
128
116
124
118
102
100
Sender 1
Sender 2
108
110

Fig. 1

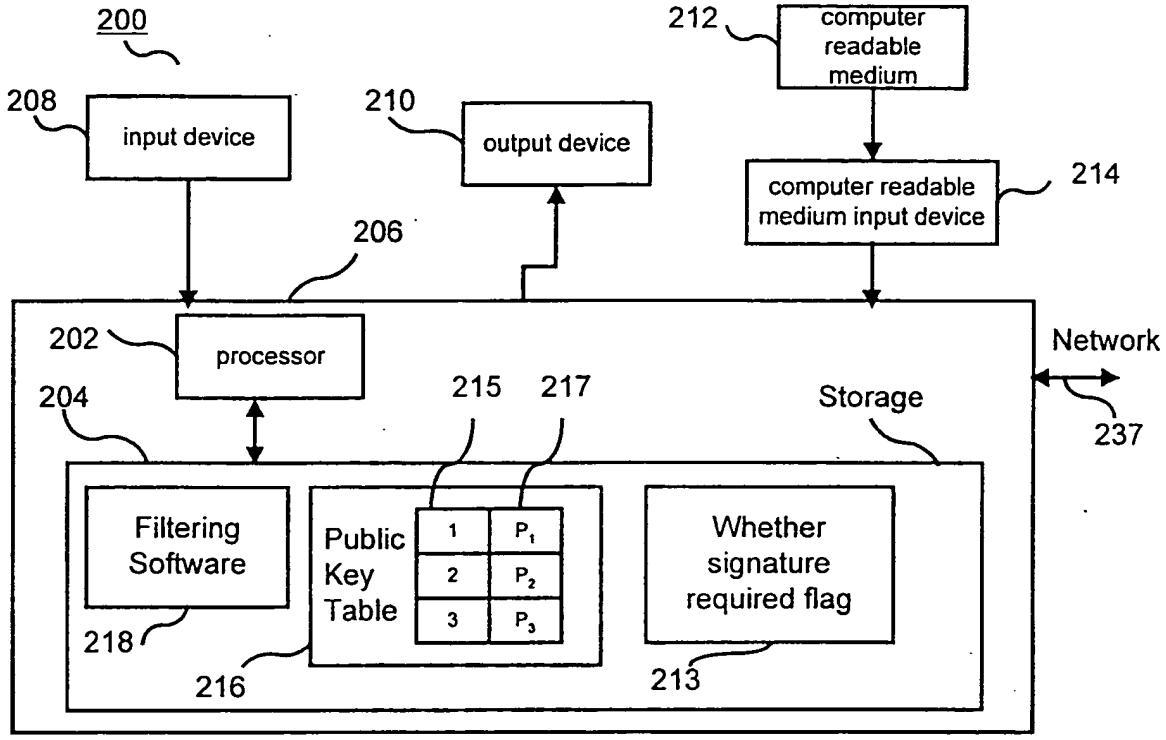


Fig. 2(a)
Router

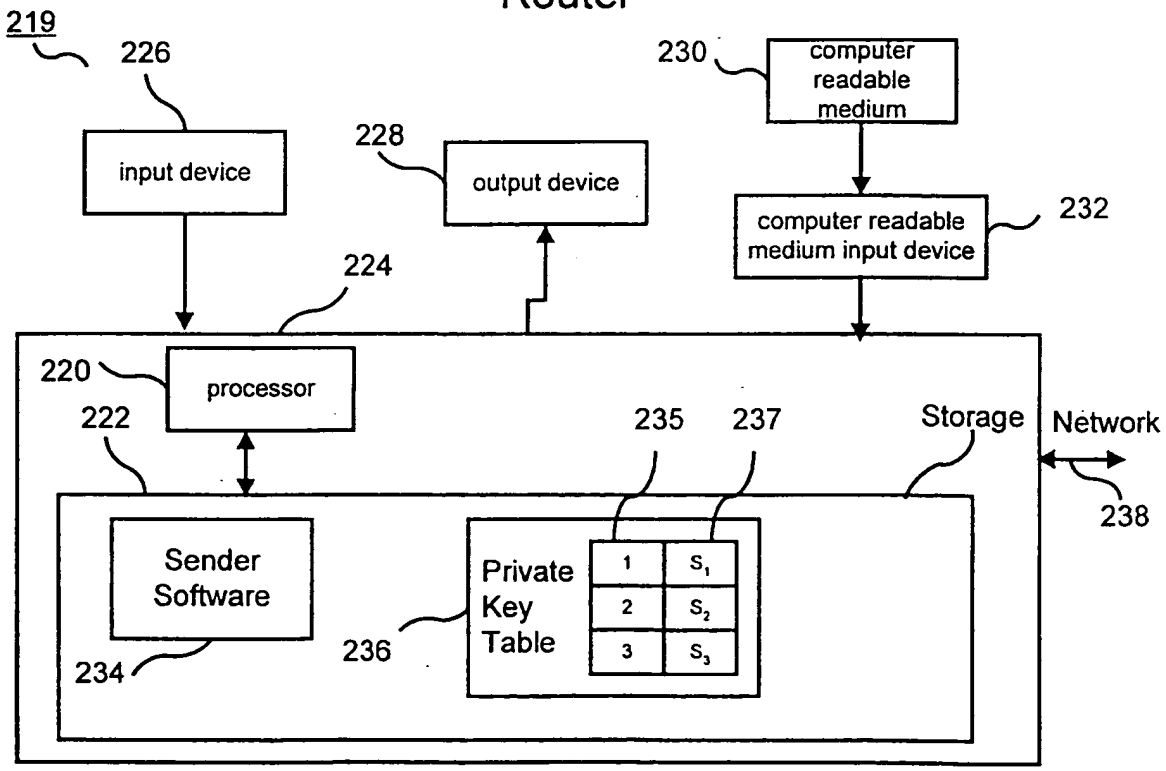


Fig. 2(b)
Sender

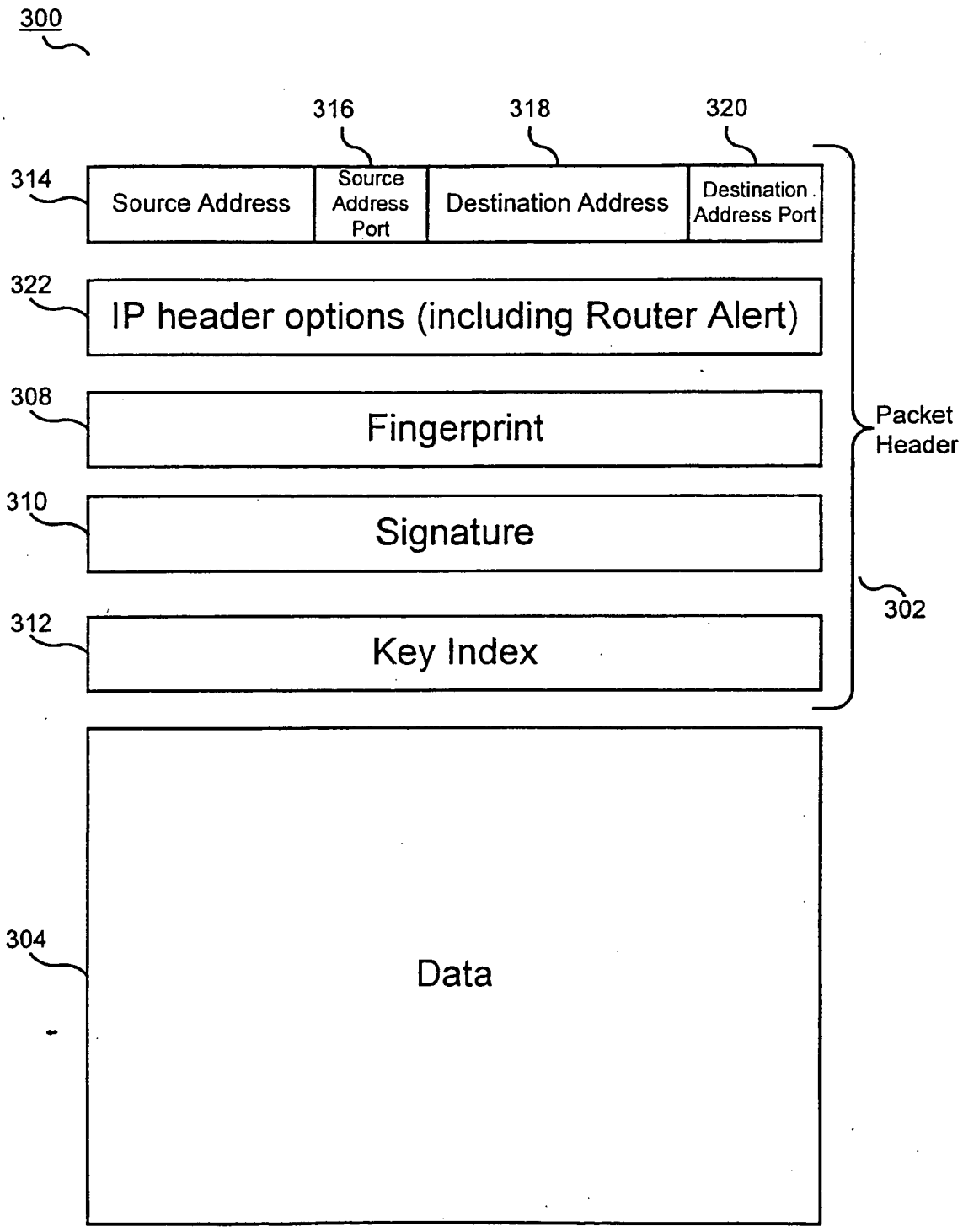

300
316
318
320
314
Source Address
Source Address Port
Destination Address
Destination Address Port
322
IP header options (including Router Alert)
308
Fingerprint
310
Signature
312
Key Index
Packet Header
302
304
Data

Fig. 3

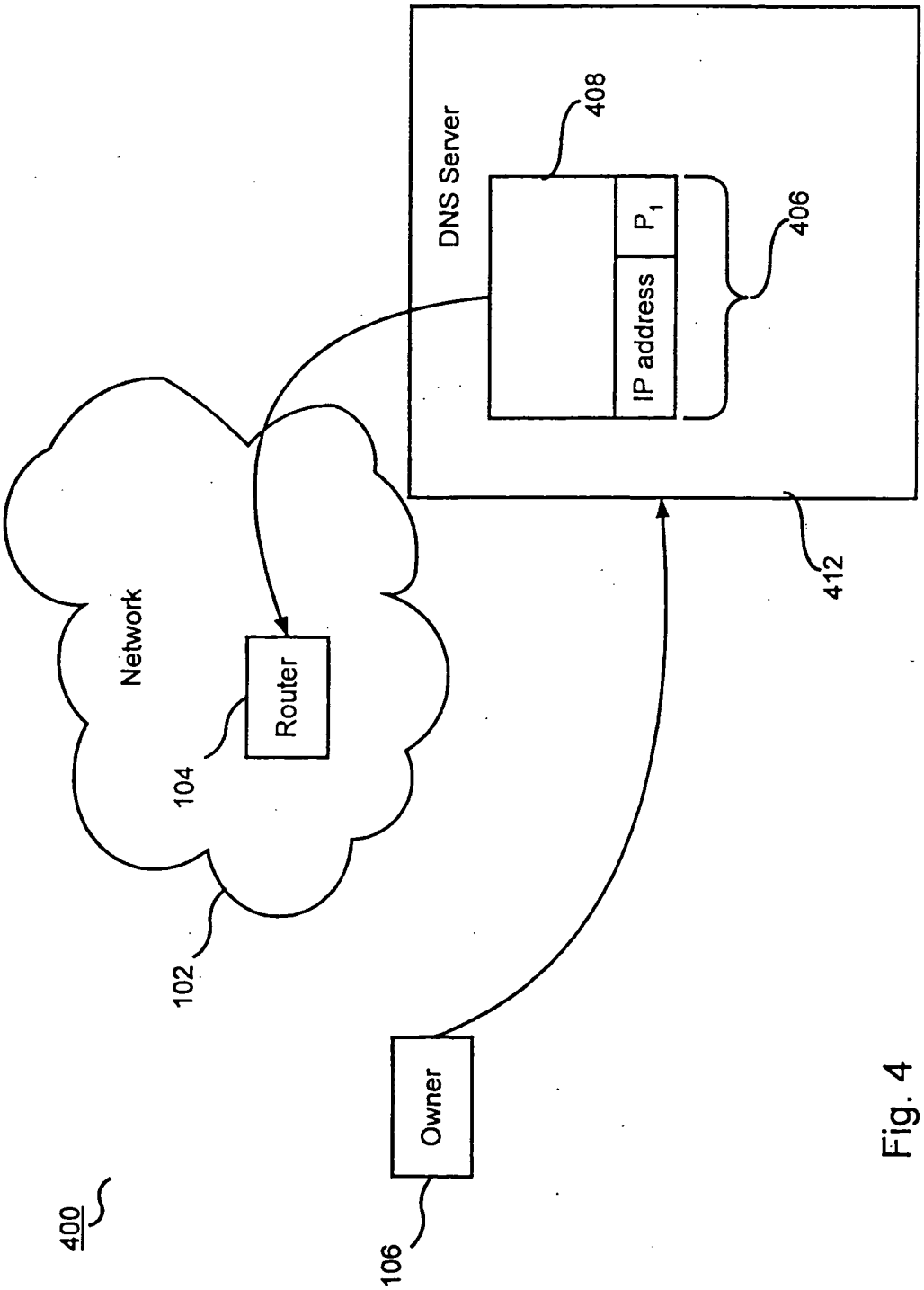

DNS Server
408
P_1
IP address
406
412
Network
Router
104
102
Owner
106
400

Fig. 4

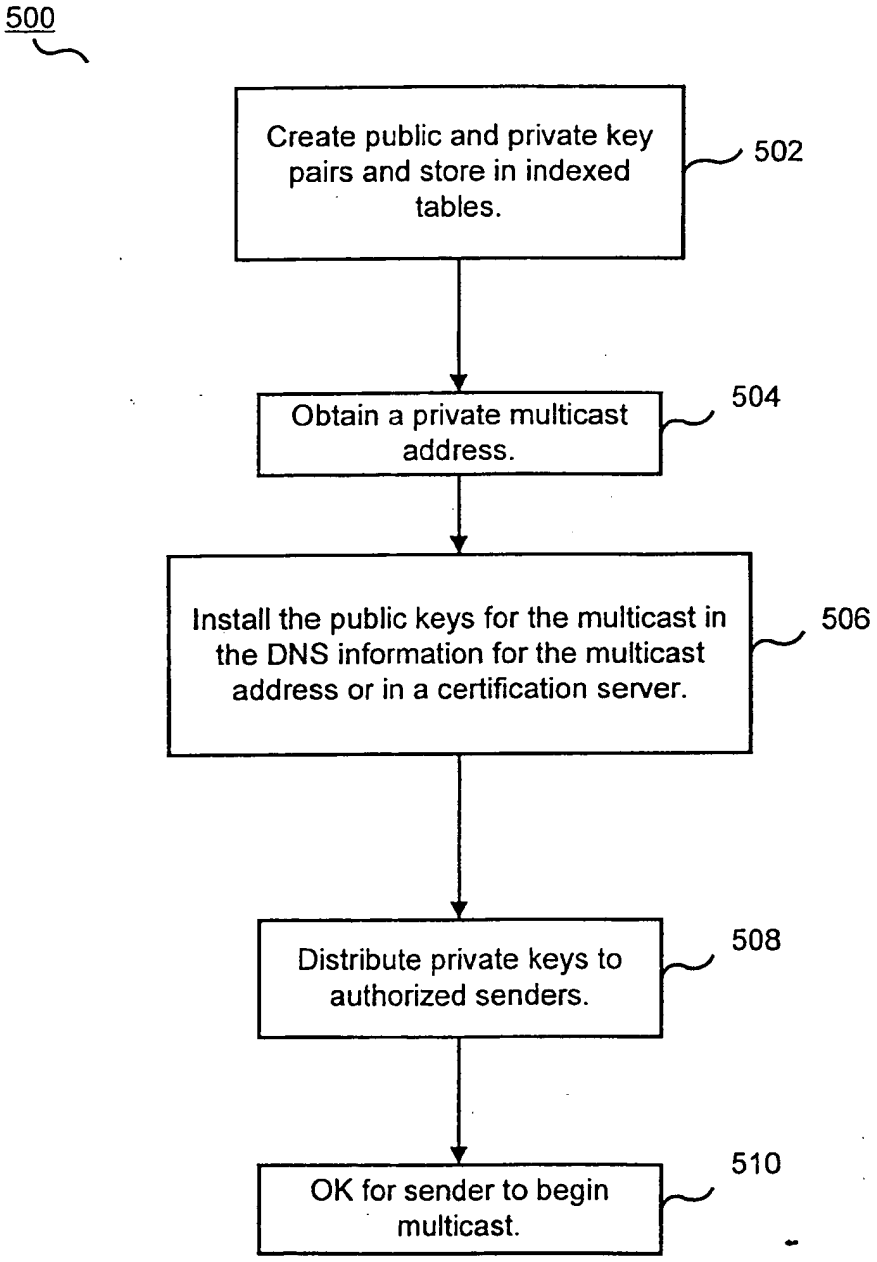


Fig. 5

Owner Distributes Keys

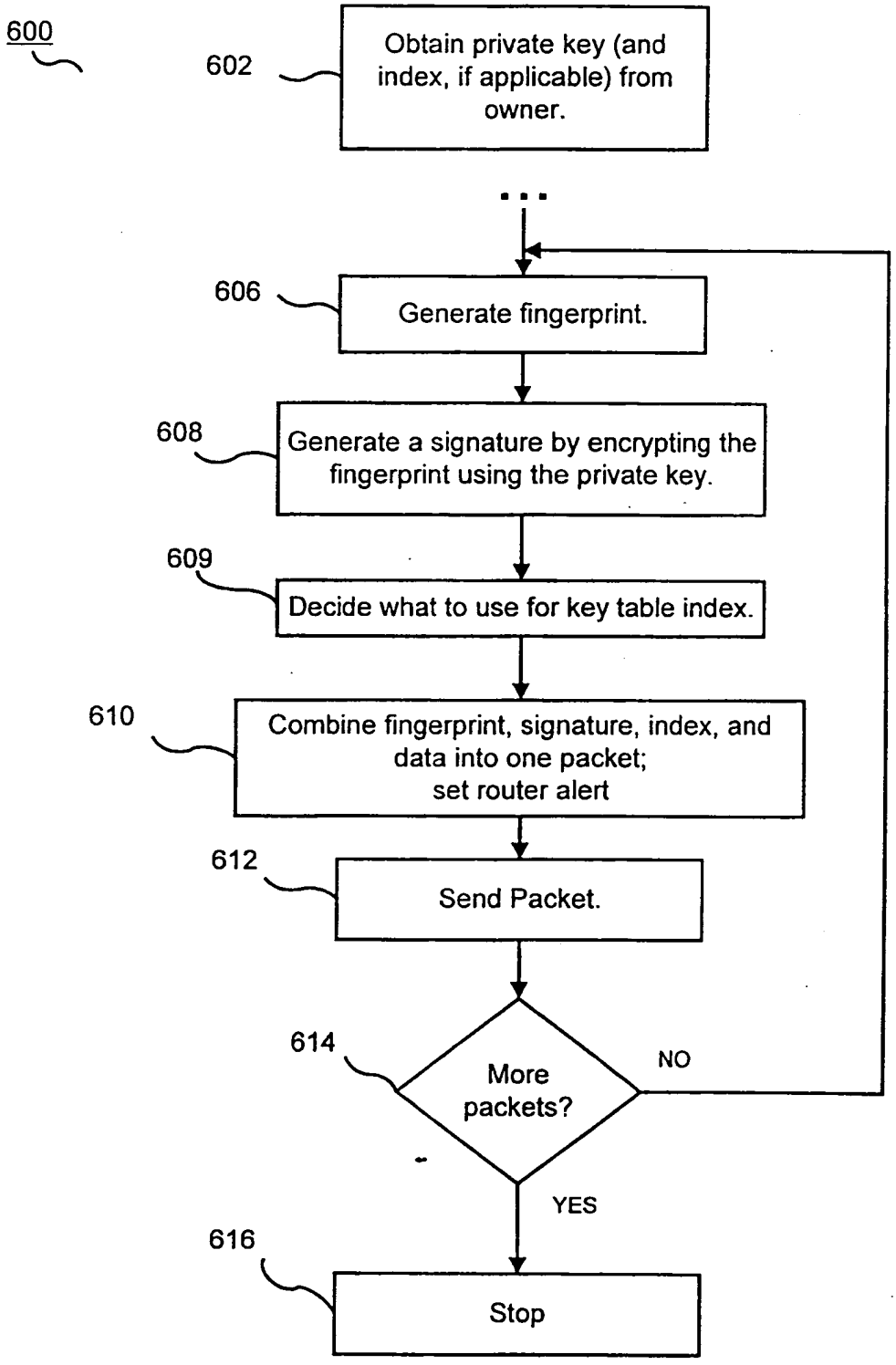


Fig. 6

Sender sends a multicast packet.

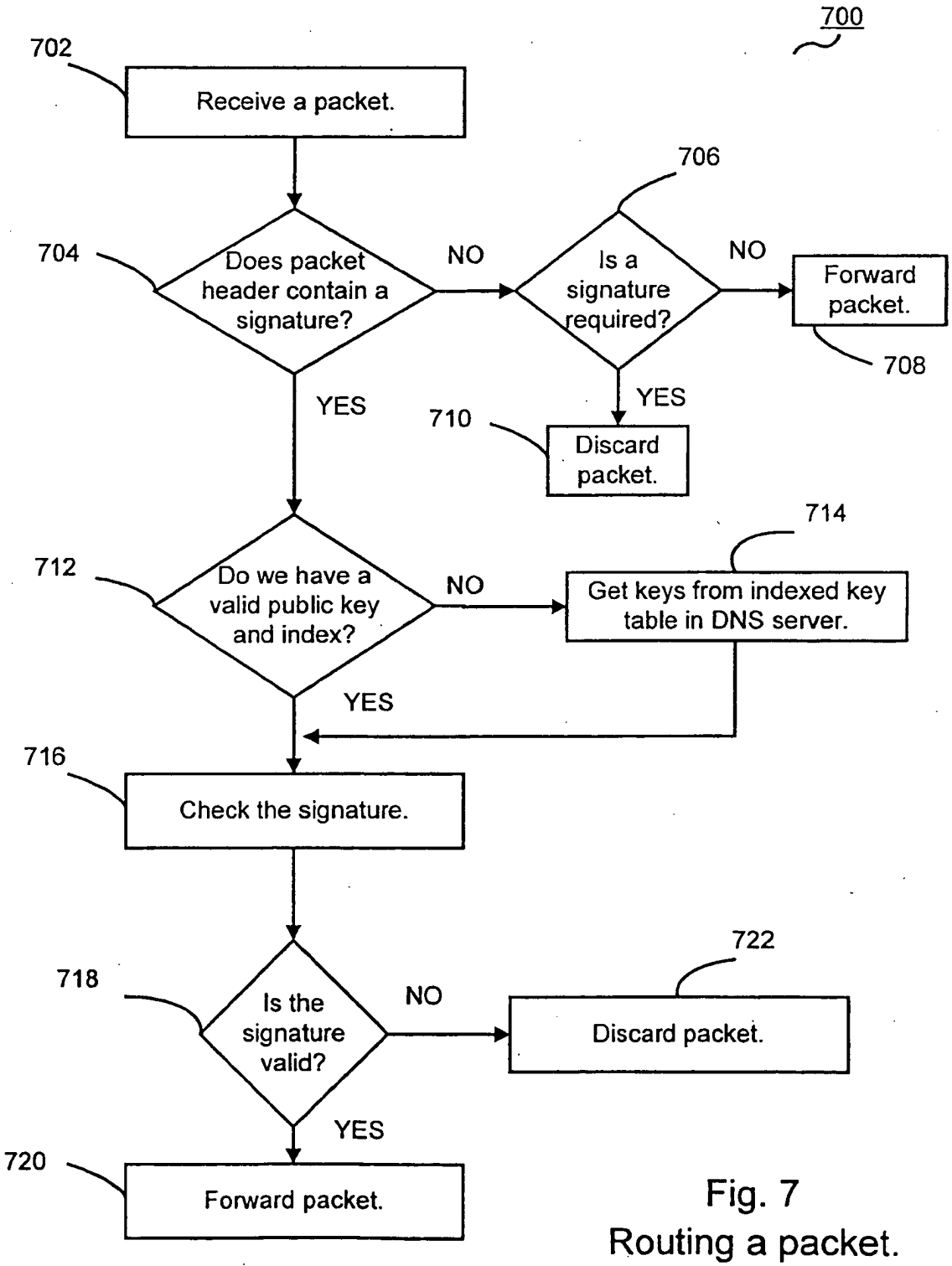


Fig. 7
Routing a packet.

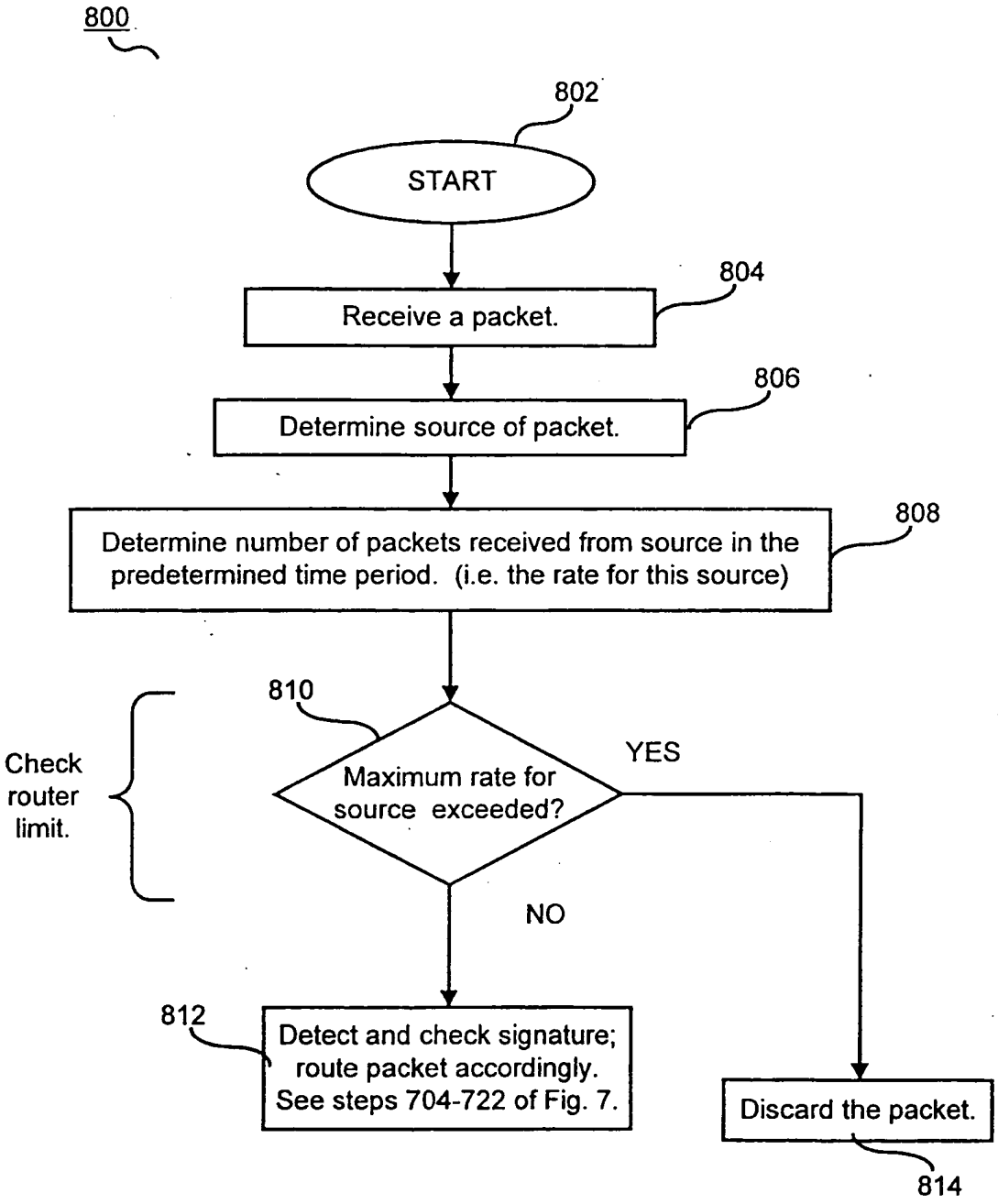


Fig. 8

Filter packets exceeding a router limit

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 99/06206

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 H04L12/22 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 00471 A (DOGON GIL ;KRAMER SHLOMO (IL); SHWED GIL (IL); ZUK NIR (IL); BEN R) 3 January 1997 see abstract see page 4, line 1 - page 7, line 18 see page 11, line 1 - line 20 see page 14, line 1 - line 5 see page 19, line 20 - line 32 see page 27, line 6 - line 26 see page 31, line 5 - page 32, line 29 see page 35, line 1 - line 23 see figures 3,14,16-21	1-4,6,7, 13-16, 18,19, 26-29, 31,32, 38-41, 43,44, 50-54
A	-/--	10-12, 22-24,

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 July 1999	12/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Poggio, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter . nal Application No
PCT/US 99/06206

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
		35-37, 47-49
A	SMITH B R ET AL: "SECURING THE BORDER GATEWAY ROUTING PROTOCOL" COMMUNICATIONS: THE KEY TO GLOBAL PROSPERITY. GLOBECOM 1996 GLOBAL INTERNET 96 CONFERENCE RECORD, LONDON, NOV. 18 - 22, 1996, vol. SUPP, 18 November 1996, pages 81-85, XP000741677 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see abstract see paragraph 1 - paragraph 2 see paragraph 4 ---	5,17,30, 42,55-58
A	WO 96 13113 A (SECURE COMPUTING CORP) 2 May 1996 see abstract see page 7, line 13 - page 11, line 17 see figure 1 ---	5,17,30, 42,55-58
A	EP 0 464 563 A (DIGITAL EQUIPMENT CORP) 8 January 1992 see abstract see page 10, line 40 - line 45 -----	8,9,20, 21,33, 34,45,46

1

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter nal Application No
PCT/US 99/06206

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9700471 A	03-01-1997	US 5606668 A	25-02-1997
		AU 6135696 A	15-01-1997
		CA 2197548 A	03-01-1997
		EP 0807347 A	19-11-1997
		JP 10504168 T	14-04-1998
		NO 970611 A	15-04-1997
		US 5835726 A	10-11-1998
		CA 2138058 A	16-06-1995
		EP 0658837 A	21-06-1995
		JP 8044642 A	16-02-1996
WO 9613113 A	02-05-1996	US 5864683 A	26-01-1999
		AU 3888595 A	15-05-1996
		EP 0787397 A	06-08-1997
EP 0464563 A	08-01-1992	US 5086469 A	04-02-1992
		CA 2045931 A,C	30-12-1991
		DE 69125757 D	28-05-1997
		DE 69125757 T	18-12-1997